The Palestinian-Israeli CYBERWAR

Colonel Patrick D. Allen, U.S. Army Reserve, and
Lieutenant Colonel Chris Demchak, U.S. Army

Cyberwar is warfighting's next frontier—combat that takes place in an ethereal electronic dimension of zeros and ones. Colonel Patrick D. Allen and Lieutenant Colonel Chris C. Demchek chronicle recent cyberskirmishes and discuss measures that the United States can take to win in cyberspace.

The current onslaught of cyber attacks against Israel's key websites is perhaps the most extensive, coordinated, malicious hacking effort in history.

— Peggy Weigle, CEO of Sanctum Inc.[1]

[This] is just a taste of things to come.

— James Adams, CEO of iDefense.[2]

IN SEPTEMBER 2000, Israeli teenage hackers created a website to jam Hezbollah and Hamas websites in Lebanon. The teenagers launched a sustained denial of service attack that effectively jammed six websites of the Hezbollah and Hamas organizations in Lebanon and of the Palestinian National Authority. This seemingly minor website attack sparked a cyberwar that quickly escalated into an international incident. Palestinian and other supporting Islamic organizations called for a cyber Holy War, also called a cyber-Jihad or e-Jihad.[3] Soon after, hackers struck three high-profile Israeli sites belonging to the Israeli Parliament (the Knesset), the Ministry of Foreign Affairs, and an Israeli Defense Force information site.[4] Later, hackers also hit the Israeli Prime Minster's Office, the Bank of Israel, and the Tel Aviv Stock Exchange.[5]

Although the long-term effects of the Palestinian-Israeli cyberwar are relatively minor and never presented a serious physical threat to any of the nations involved, the elements of the conflict are significant because they serve as a model for future cyber conflicts.

The U.S.-China cyber skirmish of May 2001 shared similar features to the Palestinian-Israeli incident. Today it is largely forgotten that during the attack hackers came close to disrupting electricity transmissions in California.[6] Had they succeeded, the cost to Californians and to the United States in national prestige and security is difficult to estimate. Chinese hackers successfully penetrated a test network of a California electric power transmission company.[7] The lessons from these early cyber conflicts need to be learned to properly understand and prepare for the inevitable cyber component of future conflicts.

The Cycle of Cyber Conflict

The Palestinian-Israeli Hacker Conflict began in 1999, but dramatically increased following the unrest of 28 September 2000. By the end of January 2001, the conflict had struck more than 160 Israeli

and 35 Palestinian sites, including at least one U.S. site. From July 1999 to mid-April 2002, 548 Israeli domain (.il) websites were defaced out of 1,295 defacements in the Middle East, and additional sites were subjected to severe denial of service attacks.[8]

The two main types of attacks were website defacement and distributed denial of service (DDoS). Website defacements tend to focus on high-profile political sites, such as government websites. In some cases, commercial transactions were curtailed for days because of repeated website defacements.[9] Broadcast servers that hackers used to launch attacks from one side were frequently used by the opposing side to launch a similar type of attack.[10] Code used to attack sites on one side was rewritten by the opposing side, which then launched a counterattack.[11] The DDoS attacks shut down opposing sites for days and added to the strain on the Internet infrastructure in the region.[12]

One pro-Palestinian hacker by the name of Dodi defaced an Internet service provider (ISP) for Israeli senior citizens and left a message claiming that he could shut down the Israeli ISP NetVision, which hosts almost 70 percent of all the country's Internet traffic. . . . The Israeli Internet Underground (IIU), a group of hackers who banded together to help increase the security of Israeli websites, claims there is already evidence of phase-four attacks. This includes the destruction of business sites with e-commerce capabilities, which the IIU believes caused an 8 percent dip in the Israeli Stock Exchange.

Attacks were also made against companies providing telecommunications infrastructure such as AT&T, which was reportedly hired to help increase the bandwidth of targeted Israeli sites.[13] One pro-Palestinian hacker by the name of Dodi defaced an Internet service provider (ISP) for Israeli senior citizens and left a message claiming that he could shut down the Israeli ISP NetVision, which hosts almost 70 percent of all the country's Internet traffic.[14]

On about 8 November 2001, Unity, a Muslim extremist group with ties to Hezbollah, announced that it had begun phase three of a four-phase strategy. Phase one focused on crashing official Israeli government sites. Phase two included attacks on the Bank of Israel and the Tel Aviv Stock Exchange. Phase three included targets such as the Israeli ISP infrastructure and the site for Lucent and Golden Lines, an Israeli telecommunications provider. Unity stated that it would hold off on the fourth and final phase, namely the destruction of Israeli e-commerce sites, threatening millions of dollars of losses in transactions.[15]

The Israeli Internet Underground (IIU), a group of hackers who banded together to help increase the security of Israeli websites, claims there is already evidence of phase-four attacks. This includes the destruction of business sites with e-commerce capabilities, which the IIU believes caused an 8 percent dip in the Israeli Stock Exchange.[16]

Although sporadic hacking has occurred between U.S. and Chinese hackers over the last few years, the collision of the U.S. EP-3 reconnaissance aircraft with a Chinese F-8 interceptor sparked the main conflict. Chinese hackers increased their activity against the United States and attempted to organize a major hacking effort during the first week in May 2001.[17]

Similar to the Palestinians, the Chinese created a website from which volunteer hackers could obtain the tools and techniques necessary to launch the "USA Kill" program.[18] The U.S. National Infrastructure Protection Center (NIPC) announced a warning on 26 April 2001 to all U.S. government and commercial websites.[19] Meanwhile, U.S. hackers, incensed by the prolonged holding of the EP-3 crew in China, began organizing the "China Killer" program.[20] By the time Chinese hackers declared a truce, they claimed to have defaced or denied service to more than 1000 U.S. websites. Pro-U.S. hackers apparently caused a similar amount of damage to Chinese websites.

Four Phases of Future Cyber Conflicts

Cyber conflicts will—

- Involve an initial period of surprise, followed by a much longer period of adaptation and recovery.
- Escalate rapidly and broaden as attackers seek vulnerable targets.
- Develop rapidly into international conflict as volunteer hackers align themselves with, or against, the various factions.
- Increase the pace of cyber arms development and proliferation.

Based on observations of the conflicts between Palestine and Israel and China and the United States, we believe future cyber conflicts will occur in four phases.

Jerusalembooks.com, Israel's largest on-line book provider, was shut down for days because of a web-defacement attack. The firm faced days of lost sales and the risk of a prolonged lack of consumer confidence in the security of on-line transactions. In a similar manner, the Israeli Land Administration Office's website was shut down for months.

Phase I: Surprise and adaptation. The Palestinian-Israeli cyberwar is an excellent example of how a nation can be surprised by a cyber attack. The Israeli teenage hackers initially surprised pro-Palestinian websites with their DDoS attacks. When the Palestinians declared a cyber-jihad against Israel, the pro-Palestinian hackers achieved an equal level of surprise against the targeted Israeli websites. The Israelis were surprised that their own citizens had initiated the cyber conflict. They also were surprised by the magnitude of the pro-Palestinian response and by the vulnerability of their government and civilian sites. After the initial shock, each side went through a period of repairing system damage and improving defenses against future attacks.

The initial effects of the conflict are worth considering. Jerusalembooks.com, Israel's largest online book provider, was shut down for days because of a web-defacement attack. The firm faced days of lost sales and the risk of a prolonged lack of consumer confidence in the security of on-line transactions.[21] In a similar manner, the Israeli Land Administration Office's website was shut down for months.[22] For Israel as a whole, such shutdowns created a lack of confidence. In addition, the large number of DDoS attacks (more than 115 in the region between 6 October and 2 December 2000) strained the Middle East's already sparse Internet infrastructure.[23]

The ultimate cost of cyber attack is generally greater to commercial targets than it is to government sites. As stated by Lawrence Gershwin, the CIA's top technology adviser, in congressional testimony, "Our 'wired' society puts all of us—U.S. business, in particular, because they must maintain an open exchange with customers—at higher risk from enemies."[24]

When a government site goes down or is defaced, the nation might lose some face. But when a company's website is shut down, it loses revenue. Matt Krantz and Edward Iwata in a *USA Today* article stated, "Some businesses lose $10,000 to several million dollars a minute when networks go down. . . . They lose, on an average, $100,000 an hour in lost productivity."[25] Reality Research estimated that businesses worldwide stood to lose more than $1.5 trillion last year as a result of cyber assaults.[26]

Even though commercial sites have a vested interest in defending against cyber attack, the drive for cost effectiveness leads most companies to ignore their website's vulnerabilities until they are hacked.[27] Therefore, there is a need to create major incentives for businesses to be secure in cyberspace, and there should be penalties for not being secure by a specific date.

Phase 2: Rapid horizontal escalation. The Palestinian-Israeli cyber conflict broadened quickly. Four weeks into the conflict, pro-Palestinian hackers struck a U.S. website. Three weeks later, Israeli hackers struck websites in Iran and Lebanon.[28] Since Israel had more websites from which to launch a counter cyber attack than did the Palestinians, the Israeli hackers began seeking vulnerable

sites outside the Palestinian National Authority and Lebanon. For example, an Israeli hacker group calling itself "the Mossad" defaced the Iranian president's website, claiming Iran was a supporter of Lebanon-based terrorist organizations.

Cyber warfare escalates horizontally and more rapidly than in standard warfare for three reasons. First, the main criteria for civilian hacker attacks appear to be vulnerability as opposed to criticality. The search for vulnerable targets expands until one is found. If government and commercial sites in the target nation are not sufficiently vulnerable, then target sites in other nations friendly to the target nation will be struck. Conversely, professional hackers in the employ of a specific nation are likely to escalate only as necessary to obtain the desired effect on the target nation.

The more bipolar a conflict, such as the Arab-Israeli conflict, the greater the chance that it will attract volunteers to one side or the other. Each side perceives the other as having permanent allies that will always back their enemies. Therefore, the United States was declared a target with Israel shortly after the Palestinian-Israeli cyber conflict began. . . . The degree of international participation observed in cyber conflicts has striking parallels to the volunteerism seen during the Spanish Civil War, a precursor to World War II.

Second, international hacker groups view the situation as one in which they can wield power without fear of retaliation. Many hackers want to show they support a cause. Since the Web includes built-in public dissemination methods, hacking into any target on the Web tends to gain some notoriety.

Third, cyber conflicts so far have been polarized, or bipolar. The more bipolar a conflict, such as the Arab-Israeli conflict, the greater the chance that it will attract volunteers to one side or the other. Each side perceives the other as having permanent allies that will always back their enemies. Therefore, the United States was declared a target with Israel shortly after the Palestinian-Israeli cyber conflict began.[29]

Traditionally, allies of a warring nation were relatively safe from military attack unless they were brought directly into the fighting. The cost of bringing a neutral nation into the fighting usually incurred at least some penalty on the nation choosing to escalate. In cyberspace, however, the cost of escalation is small for a nation, and almost nonexistent for an individual hacker. Therefore, rapid horizontal escalation will likely occur in future cyber conflicts.

Phase 3: Rapid nonstate internationalization. Cyber conflict tends to attract two types. The first type includes groups of talented hackers who are frequently involved in international cyber incidents. The second consists of amateur hackers attracted through patriotic or ideological fervor. The Palestinian-Israeli cyber conflict attracted hackers from Israel, Palestine, Lebanon, Germany, Saudi Arabia, Pakistan, Brazil, and the United States. Most of the attacks against Israel were launched from outside Israel or the Palestinian National Authority.[30] Of note is that one or more Brazilian hacker groups attacked both sides in the Palestinian-Israeli conflict, apparently trying to show up each side's participants. The U.S.-China cyber skirmish attracted pro-U.S. hackers from the United States, Saudi Arabia, Pakistan, India, Brazil, Argentina, and Malaysia. Pro-Chinese hackers were attracted from China, Japan, Indonesia, and Korea. Note that the alignments of the hackers did not necessarily match the desires of the nation, except in those nations where the government tightly controls the Internet.

The degree of international participation observed in cyber conflicts has striking parallels to the volunteerism seen during the Spanish Civil War, a precursor to World War II. This conflict between fascists on one side and communists and democrats on the other drew large numbers of foreign volunteers to both sides. In both the Spanish Civil War and the Palestinian-Israeli cyber conflict, ideology,

not profit, motivated volunteers. Mercenary hackers exist, but they were not reported as being active in either the Palestinian-Israeli or the U.S.-China cyber conflicts.

Most hackers involved in either the Palestinian-Israel or U.S.-China cyber conflicts were veterans of previous international cyberwars. The Pakistani hackers, for example, were also involved in defacing Indian websites, and Brazilian hackers were involved in defacing U.S. sites.[31] "Hactivism" is tempting when hackers have the power to participate on the international scene.[32]

One hacker, or a small group of hackers, can do a lot of damage in short order. During the U.S.-China cyber conflict, a hacker group named "PoizonB0x" successfully hacked more than 400 Chinese (*.cn) websites.[33] One report estimated there were only 30 core hackers in the Palestinian-Israeli conflict who provided the tools, while the volunteer script kiddies provided the "brute force" checks, scanning potential target sites for vulnerabilities.[34] The brute force search of 209-series IP addresses allowed Chinese hackers to discover the presence of an unsecured electric power transmission test network in California.[35]

One hacker, or a small group of hackers, can do a lot of damage in short order. During the U.S.-China cyber conflict, a hacker group named "PoizonB0x" successfully hacked more than 400 Chinese (*.cn) websites. One report estimated there were only 30 core hackers in the Palestinian-Israeli conflict who provided the tools, while the volunteer script kiddies provided the "brute force" checks, scanning potential target sites for vulnerabilities.

Even if the initial cyber strike of a future conflict is a well-coordinated military action, volunteers from many nations will likely be involved in copycat attacks, complicating real-war combat operations. This threat alone has numerous implications for national sovereignty and international law.

Phase 4: Global Learning and Increased Cyber Arms Development and Proliferation. Hacking tools used and improved in the Palestinian-Israeli cyberwar soon appeared in other international and domestic hacks. During the Palestinian-Israeli cyberwar, Israeli hackers developed a new type of DDoS attack tool. Teenage hackers in the United States acquired this attack tool from Israeli hackers and planned a worldwide attack on the Internet to take place on New Year's Day 2001. Had the FBI not been alerted to the plot, the attack might have succeeded in seriously disrupting the Internet on New Year's Day.[36]

During the U.S.-China cyber skirmish, the Carko DDoS attack was launched.[37] Not only did a Carko DDoS agent attempt to crash the target system, it used a buffer overflow attack to enter a new root password, or it installed a back door in the target system while the target system was recovering from the attack. This meant systems that were brought down by Carko attacks needed to be checked for software that would allow later penetrations.

Although DDoS attacks were known and used before this conflict, the ability for one person with limited bandwidth to undertake a large-scale DDoS attack is a fairly recent development. This type of DDoS attack can use a 56-kilobyte modem and an asymmetric digital subscriber line (ADSL) to begin an attack, which is then magnified 10,000 times by net service broadcasters to generate attacks of the magnitude of two thirds of a T1 line. "With tools like these, a 56-kilobyte modem can become a powerful weapon and your bandwidth is irrelevant," notes Ben Venzke, of iDefense.[38] A few coordinated laptop attacks through modems, therefore, can generate a combined attack equal to several T1 lines or even a T3 line. Such an attack can swamp most systems.

In addition to DDoS attacks launched through broadcast sites, there is also a technique whereby hackers place software on other Internet servers and later trigger it at a particular time. These infected servers are called zombies in that they mindlessly participate in DDoS attacks. The FBI discovered that 560 servers at 220 Internet sites had been infected for use in a single widespread DDoS attack.[39]

Overall, the rate of cyber arms development tends to increase during cyber conflicts, just as weaponry

develops faster during war. What is more challenging, however, is that the rate of proliferation of cyber arms is much faster than the proliferation of traditional arms.

Policy Implications

Based on these events, there are four national and international policy needs:

1. To decide who will provide security on the Web.
2. To provide legal responses to rapid horizontal escalation.
3. To enforce legal responsibility for hacker citizens responsible for international incidents.
4. To halt proliferation of cyber arms.

Who will provide security on the Web. The main policy question associated with the cost of doing business on the Web is, "Who is responsible for securing the Web?" Is it the large ISP? Corporations? The government? Or will the Internet remain a free-fire zone?[40]

Some nations have chosen to assign Web security to the government, especially in nations where the Internet is considered a threat to the government's absolute control, such as in China. Most European nations are passing laws that place the government as the central guarantor of Web security. As economies and communications rely more on the Internet, nations will make choices that place them somewhere along the spectrum of security versus privacy. In most cases, laws will ensure the security of the Web at the cost of personal privacy.[41] The United States will need to decide where on this spectrum it will operate and what level of cyber security it will need to provide to support secure transactions and a measure of privacy.

Legal response to rapid horizontal escalation. The higher a cyber conflict's visibility, the more it will attract international hackers, and the sooner hackers will seek out vulnerable sites. What are the legal options of a nation attacked in a conflict in which it is not involved? For a legal response, the identity of the perpetrator must be established. However, cyber attacks are not launched frequently by a nation, but by private citizens. It is difficult to justify a retaliation bombardment against hackers who violate their own nation's neutrality or allegiance with an attacked country. Hacking is an asymmetric threat from nonstate actors that makes justified retaliation difficult.

During the U.S.-China cyber skirmish, the Carko DDoS attack was launched. Not only did a Carko DDoS agent attempt to crash the target system, it used a buffer overflow attack to enter a new root password, or it installed a back door in the target system while the target system was recovering from the attack. This meant systems that were brought down by Carko attacks needed to be checked for software that would allow later penetrations.

Little can be done in cyberspace to admitted hackers because they do not present a ready target. Individual hackers or hacker groups do not tend to own infrastructure that can be targeted, even in cyberspace. When such infrastructure exists, getting legal access to it is difficult because of national sovereignty. For example, when the United States performed a sting operation against two Russian hackers, issues of due process arose because of the FBI's long-distance electronic search of the hacker's computers in Russia.[42] Any response must consider the possible collateral damage potentially caused by such retaliation. Since hackers tend to route their attacks through many third-party servers, any cyber retaliation must consider the fact that the counterattack might fall on the servers of innocent bystanders.

Overall, nations need to define their legal authority to exercise sovereignty, prosecute, and impose penalties on hackers convicted of cyber attacks. International agreements not to harbor hijackers contributed to a significant decrease in such events. Similar international agreements regarding cyberspace crime could help reduce the sanctuaries available to hackers.

Legal responsibility. Every nation must face the fact that its citizen hackers can cause international incidents not in its best interest. Israel was dragged into a cyber conflict by its own teenage hackers, not as a government decision. Israel was not prepared

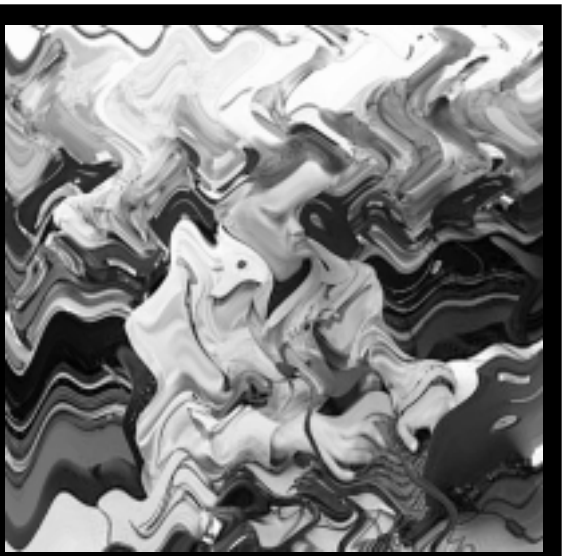
to wage a cyberwar and was more vulnerable than its opposition.

Cyber violations of online externally connected networks lie in a gray area of international and domestic security laws. To locate and prosecute hackers, nations must rely on the authorities and laws of the hacker's host nation. Israel estimated that damage caused by the globally distributed "Love" virus, including the disruption of national cellular phone companies, reached $12 million. However, Israel could not file criminal charges against the hacker because his home country (the Philippines) did not make virus writing a criminal offence until after the event.[43]

Criminal punishment is particularly difficult when the hackers operate from a blatantly hostile nation. However, nations have certain rights under an internationally recognized protective principle if offending nations are not helpful. There is international case law, albeit limited, that might support state action in response to cyber attacks. Under this principle, when a person from country A harms country B, and country A does not prevent that person from continuing to do harm, then country B has the right to take action against country A.[44] Although this principle has not yet been applied in cyberwar cases, the legal precedence exists.

If a nation intends to treat hackers as criminals and terrorists, then its policy will be designed to squash all hacker activities, however mild. Such a policy is sure to alienate its hacker citizens. Judging from their proposed cyber laws, most European nations appear to be heading in this direction.[45]

The United State is less likely to crack down severely on domestic hackers. Such a crackdown would not only be unnecessary, but counterproductive. An option more likely to succeed is to provide incentives for white-hat hackers. These hackers have an interest in helping others and do no damage. White-hat hackers could be encouraged to locate vulnerabilities and help system administrators apply the necessary patches. Government or private security agents could verify that the patch is correct and does not include a back door. White-hat hackers could be publicly rewarded and brought in as independent evaluators of other white-hat solutions. White-hat hackers should be rewarded and their work confirmed, but they should not necessarily be controlled or officially employed by the government. The image of independence, as well as doing good, has great appeal among white-hat hackers.



Every nation must face the fact that its citizen hackers can cause international incidents not in its best interest. Israel was dragged into a cyber conflict by its own teenage hackers, not as a government decision. . . . If a nation intends to treat hackers as criminals and terrorists, then its policy will be designed to squash all hacker activities, however mild. Such a policy is sure to alienate its hacker citizens. Judging from their proposed cyber laws, most European nations appear to be heading in this direction. . . . An option more likely to succeed is to provide incentives for white-hat hackers [who] have an interest in helping others and do no damage.

Conversely, black-hat hackers need to be identified and prosecuted. The legal system needs to develop the full range of formal sanctions against hacking, cracking, and carding that vary according to the socially unacceptable effects of these activities. At present, federal and state agencies in the United States are woefully unqualified to handle the degree and volume of hacks.[46] A major difficulty is that the government has difficulty attracting and retaining skilled computer specialists because of the poor salary it offers.[47]

One approach might be to use white-hats to hunt down black hats in cyberspace. Elite military forces dedicated to averting, diverting, derailing, tracking, and punishing major hacks against U.S. and global interests might keep order on the Web and keep cyber conflicts from escalating.[48]

International Response

Every cyber skirmish sparks the development of new cyber arms, which are then rapidly disseminated to professional and amateur hackers around the globe. Proliferation has significant implications for

monitoring hacking tools used in conflicts and in new Web technologies in general. In addition to monitoring the capabilities of these new tools, nations need to monitor the chats of amateur hackers who cannot resist trying out the power of the new toy. (Hackers sponsored by a nation will not use the new weapon unless it is part of an overall plan, so that the surprise element is not wasted.) Therefore, each nation needs to develop countermeasures to help preclude the use of the new cyber weapon or to mitigate its effects. Scanning servers for zombie software that allows DDoS attacks to be launched needs to be performed regularly to minimize the magnitude of future attacks. By keeping abreast of new hacking tools and methods, a nation can be better prepared to preclude or mitigate their effects.

In any modern conflict, cyberspace can be an additional avenue of attack. Because the United States is the largest player in the international political environment, it has become a lightning rod for hacking and terrorist attacks, regardless of whether the nation was involved in the initial conflict. Until 11 September 2001, the United States was fairly complacent about its enemies overseas. However, the distance between the United States and its enemies is dramatically reduced. The lessons from early cyber conflicts need to be learned now to properly prepare for future conflicts. ***MR***

NOTES

1. Peggy Weigle, Corporate Executive Officer (CEO), Sanctum Inc., quoted in Carmen J. Gentile, "Hacker War Rages In Holy Land," on-line at <www.wired.com/news/politics/ 0,1283,40030,00.html>, 8 November 2000.
2. James Adam, CEO, iDefense, quoted in Gentile, "Israeli Hackers Vow to Defend," on-line at <www.wired.com/news/politics/ 0,1283,40187,00.html>, 15 November 2000.
3. "Cyber War also Rages in MidEast," *The Associated Press,* on-line at <www.wired.com/news/print/0,1294,39766,00.html>, 26 October 2000; Brian Krebs, "Hackers Worldwide Fan Flames in Middle East Conflict," on-line at <www.infowar.com/hacker/00/ hack_112000c_j.shtml>, 20 November 2000.
4. "Cyber War Also Rages in MidEast."
5. Krebs, "Hackers Worldwide"; Infowar.com, 20 November 2000; "Israel's 'Mossad' Hackers Break into Iranian President's Website," *Xinhua News Agency Bulletin* (18 January 2001); on-line at <www.infowar.com/hacker/01/hack_011901c_j.shtml>, 19 January 2001; Tania Hershman, "Israeli Seminar on Cyberwar," on-line at <www.wired.com/news/politics/0,1283,41048,00.html>, 10 January 2001.
6. Gentile, "Palestinian Crackers Share Bugs," on-line at <www.wired.com/news/politics/0,1283,40449.00.html>, 2 December 2000.
7. Robyn Welsman, "California Power Grid Hack Underscores Threat to U.S.," on-line at ww.newsfactor.com/perl/story/11220.html>, 13 June 2001.
8. "Israel Suffers Escalating Hack Attacks," on-line at <www.mi2g.com/cgi/mi2g/press/150402.php>, 15 April 2002.
9. Gentile, "Israeli Hackers."
10. Ibid., "Palestinian Crackers."
11. Ibid., "Hacker War Wages."
12. Ibid., "Israeli Hackers."
13. Krebs; Elisa Batista, "Palestinian Group Targets AT&T," on-line at <www.wired.com/news/business/0,1367,39913,00.html>, 6 November 2000.
14. Gentile, "Israeli Hackers."
15. Ibid., "Hacker War Wages."
16. Ibid., "Israeli Hackers."
17. Michelle Delio, "It's (Cyber) War: China vs. U.S.," on-line at <www.wirednews.com/news/print/0,1294,43437,00.html>, 30 April 2001.
18. Ibid.
19. NIPC Advisory 01-009, "Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May," on-line at <www.nipc.gov/warnings/advisories/2001/01-009.htm>, 26 April 2001.
20. Delio, "U.S., Chinese Hackers Wage Online War," *Agence France Presse* (24 April 2001), on-line at <www.inq7.net/inf/2001/apr/ 24/inf_3-1.htm>, 24 April 2001.
21. Gentile, "Palestinian Crackers" and "Israeli Hackers."
22. Elazar Levin, "Overseas Hackers Strike Again: Israel Land Administration Shuts Down Most of its Web Site," *Israel's Business Arena* (4 December 2000), on-line at <http://new.globes.co.il/serveEN/globes/ docView.asp?did=454769&fid=947> and <www.infowar.com/ hacker/00/hack_120500a_j.shtml>, 5 December 2000.
23. Gentile, "Palestinian Crackers."
24. Lawrence K. Gershwin, "Cyber Threat Trends and US Network Security," statement before the Joint Economic Committee, on-line at <www.cia.gov/cia/public_affairs/speeches/gershwin_speech_062>, 21 June 2001.
25. Matt Krantz and Edward Iwata, "Companies Bleed Cash When Computers Quit," *USA Today,* 11 June 2001, section B, page 1.
26. "Israel Suffers."
27. Delio, "Got a Virus? Blame the Tightwads," on-line at <www.wired.com/news/technology/0,1282,42047,00.html>, 28 February 2001.
28. "Cyber War Also Rages"; Krebs, "Hackers Worldwide."
29. Gentile, "Hacker War Rages."
30. Ibid., "Israeli Hackers."
31. Robert MacMillan, "Hackers Deface Policy.com as 'Public Service'," *Newsbytes,* Washington, D.C., on-line at <www.infowar.com/hacker/00/hack_111500a_j.shtml>, 15 November 2000.
32. Carrie Kirby, "Hacking with a Conscience is a New Trend," *San Francisco Chronicle*, 20 November 2000,on-line at <www.infowar.com/hacker/00hack_112400a_j.shtml>, 24 November 2000.
33. John Lyman, "Hackers Aim at Computer Security Sites," on-line at <www.newsfactor.com/perl/printer/11230>, 14 June 2001.
34. Gentile, "Palestinian Crackers."
35. Welsman, "California Power Grid."
36. Krebs, "FBI Arrests Hacker in Planned New Year's Eve Attack," *Newsbytes*, Washington, DC (12 January 2001), on-line at <www.infowar.com/hacker/01/hack_011501b_j.shtml>, 15 January 2001; and "Feds Warn of Concerted Hacker Attacks on New Year's Eve," *Newsbytes,* Washington, DC (29 December 2000),on-line at <www.infowar.com/hacker/00/hack_122900a_j.shtml>, 29 December 2000.
37. Steve Gold, "More Details Emerge on Expected Chinese Hack Attacks," *Newsbytes*, Parsippany, NJ (27 April 2001), on-line at <www.infowar.com>, 27 April 2001.
38. Gentile, "Palestinian Crackers."
39. Krebs, "Feds Warn."
40. Chris C. Demchak, "State Security Paths in a Digital Mass Society: New Internet Topologies and Security Institution Obligations," *Cambridge Review of International Affairs,* special issue on state security and the Internet, date unknown.
41. Bob Sullivan, "Cybercrime Treaty Targets Hackers," *MCNBC News*, on-line at <www.msnbc.com:80/news/480734.asp>, 6 November 2000, and <www.infowar.com/hacker/00/hack_110600e_j.shtml>, 6 November 2000.
42. Thomas C. Greene, "FBI Hacked Russian Hackers," on-line at <www.theregister.co.uk/content/8/18496.html>, 25 April 2001.
43. Israeli Consulate Online Service (IsraelLine), "Love Virus Hits Israeli Businesses," New York, 8 May 2000; Lynn Burke, "Love Bug Case Dead in Manila," *Wired Online*, 21 August 2001.
44. Iain Cameron, *Protective Principle of International Criminal Jurisdiction* (Dartmouth, MA: Dartmouth Publishing Company, 1993).
45. Sullivan, "Cybercrime Treaty."
46. Greg Farrell, "Police Outgunned by Cybercriminals," *USA Today,* 6 December 2000, on-line at <www.infowar.com>, 7 December 2000.
47. Patrick Thibodeau, "CIO Panel Recommends Hiring IT Rookies," *Computerworld,* on-line at <http://iwsun4.infoworld.com/ articles/hn/sml/00/10/12/001012hnhiring.xml>, 12 October 2000.
48. Demchak, "State Security Paths."

Colonel Patrick D. Allen, U.S. Army Reserves (USAR) is Senior Lead Systems Engineer, General Dynamics Advanced Information Systems, Information Operations, Arlington. He received a B.S. in Physics, an M.S. in Industrial Engineering and Operations Research, an M.S. in Strategic Studies, a Ph.D. in Mineral Economics and Operations Research, and he is a graduate of U.S. Army Command and General Staff College (CGSC), the Army War College (AWC), and The Air War College. More than 40 of his articles, primarily on the subjects of modeling and simulation and information operations, have been published.

Lieutenant Colonel Chris C. Demchak, USAR, is cofounder of the Cyberspace Policy Research Group, a transnational group of scholars documenting and studying the global spread and effects of Web technologies in military and other national agencies. She received an M.S. in economic development, an M.S. in energy engineering, and a Ph.D. in political science with a focus on organization theory and complex systems. She has led empirical in-depth field studies of U.S., British, and Israeli armies and secondary-source analysis on democratic civil-military implications of modernization in Central European militaries. Many of her articles have been published, as well as her book Military Organizations, Complex Machines: Modernization in the U.S. Armed Services.